REMARKS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-8 are currently pending in the present application, Claims 1, 2, 5, and 6 having been amended by way of the present amendment. No new matter has been added.[1]

In the outstanding Office Action, Claims 1-8 were rejected under 35 U.S.C. § 102(b) as anticipated by Hashimoto, et al. (JP 2002-232417, hereinafter "Hashimoto").

As an initial matter, Applicants and Applicants' representatives thank Examiner Turchen for the courtesy of an interview granted on January 29, 2009. During the interview, differences between the claimed invention and the art of record were discussed. Comments discussed during the interview are summarized below.

Regarding the rejection of Claims 1-8, Applicants respectfully traverses the rejection.

Claim 1 has been amended to clarify that the tamper resistant microprocessor that executes a plurality of programs in parallel under a multi-task programming environment includes a cache memory configured to store the execution code or data decrypted by the decryption unit and ***an actual encryption key used in decrypting the execution code or data for at least one cache line***, the actual encryption key being stored in a secret protection attribute holding section ***of at least one cache line***, the execution code or data stored in the cache memory remaining even after each program terminates. Independent Claim 5 includes similar features.

As discussed during the interview, the references fail to disclose or suggest at least this feature of the amended independent claims.

The outstanding Office Action cites paragraphs 43-45 of Hashimoto as corresponding to the original Claim 1 "a cache memory configured to store the execution code or data

[1] The amendments to Claims 1, 2, 5, and 6 find support at least in Applicants' Fig. 2 and in the discussion thereof in the specification.

decrypted by the decryption unit into one of cache lines provided in the cache memory, each cache line having a secret protection attribute holding section for storing an actual encryption key used in decrypting the execution code or data, the execution code or data stored in the cache memory remaining even after each program terminates."

Further, the Official Action states in the Response to Arguments section on page 2 (regarding Claim 1) that "[t]he claim specifically states that each cache line having a secret protection attribute holding section for storing an actual encryption key, but does not state that the key is located in a physical location in the cache memory." The Official Action goes on to assert that Hashimoto includes a secret protection attribute holding section in the key value table, citing paragraphs 102 and 127.

As discussed during the interview, the examiner explained that he is interpreting "each cache line *having* a secret protection attribute holding section for storing an actual encryption key," as not positively reciting that the actual encryption key is stored in a secret protection attribute holding section of the cache memory. The examiner agreed that the present amendment clarifies and positively recites this feature.

Additionally, the examiner stated in Interview Summary Sheet that the claims, as presently amended, overcome the rejection.

Specifically, as discussed during the interview, Hashimoto describes that the encryption key is not stored in the cache memory but is, instead, stored in the key value table 804 in the lock management department 701 (see paragraph 127, and see paragraph 102 particularly regarding a data encryption key). In other words, the encryption attribute tag stores a task ID and an encryption key corresponding to the task ID is determined by referring to the key value table.

Thus, Hashimoto does not disclose or reasonably suggest "the actual encryption key being stored in a secret protection attribute holding section of at least one cache line," as recited in amended Claims 1 and 5.

Accordingly, as Hashimoto does not disclose or suggest all of the elements in independent Claims 1 and 5, it is respectfully submitted that Hashimoto does not anticipate independent Claims 1 and 5 and claims dependent therefrom.

Dependent Claims 2 and 6 were also discussed during the interview. Dependent Claims 2 and 6 are submitted to patentably define over the applied references by virtue of at least their dependency on Claims 1 and 5, respectively. Additionally, amended Claim 2 recites that "the cache memory control unit judges whether the ***contents*** of the actual encryption key stored in the secret protection attribute holding section of a cache line that stores the existent execution code or data is identical with the ***contents*** of the prescribed key stored in the key value register," and amended Claim 6 recites that "whether the ***contents*** of the actual encryption key stored in the secret protection attribute holding section of a cache line that stores the existent execution code or data is identical with the ***contents*** of the prescribed key stored in the key value register is judged." In contrast, in Hashimoto, the ***identifiers*** are compared and not the actual content of the keys (see paragraph 81). Accordingly, Claims 2 and 6 are believed to further patently define over Hashimoto.

Applicants resubmit that dependent Claims 3 and 7 patentably define over the applied references by virtue of at least their dependency on Claims 1 and 5, respectively. Additionally, Claims 3 and 7 recite "storing the prescribed encryption key stored in the key value register into the secret protection attribute holding section of a cache line for the data." In contrast, Hashimoto describes a data cache 401 storing data with the tag of a data key identifier (see [0102]). The identifiers in Hashimoto play a role in identifying individual encryption keys, but the encryption keys play a role in encrypting data (see paragraph 80).

Further, as described in paragraph [0102], a data key, corresponding to the data key identifier, is stored in not the data cache 401 but a data key table 710 (also see Fig 7). Additionally, paragraph [0045] states that the cryptographic key to be used at a time of applying the cryptographic processing on some cache data is determined by the encryption attribute tag. This means that the cryptographic key is not the same as the encryption attribute tag. Thus, for all of these reasons, Claims 3 and 7 are believed to further patently define over Hashimoto.

Applicants resubmit that dependent Claims 4 and 8 patentably define over the applied references by virtue of at least their dependency on Claims 1 and 5, respectively. Additionally, Claim 4 recites that "the cache memory control unit encrypts a processing result of the data by using the actual encryption key stored in the secret protection attribute holding section of a cache line for the data," and Claim 8 recites that "the data access control method further comprises encrypting a processing result of the data by using the actual encryption key stored in the secret protection attribute holding section of a cache line for the data." In contrast, in Hashimoto, the data is not encrypted and returned by using a key stored in the cache memory (see paragraph 102). Accordingly, Claims 4 and 8 are believed to further patently define over Hashimoto.

Consequently, in view of the present amendment and in light of the above discussions, the outstanding grounds for rejection are believed to have been overcome. The application as amended herewith is believed to be in condition for formal allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Ronald A. Rudder, Ph.D.
Registration No. 45,618

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)